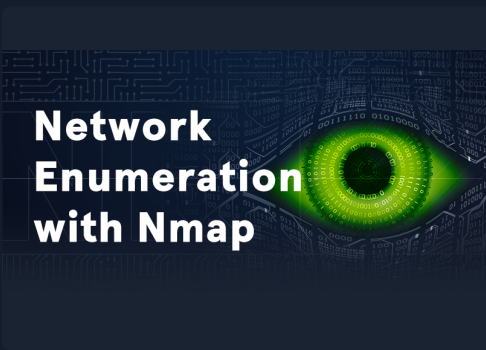


Targets compromised: 248

Ranking: Top 5%

MODULE

PROGRESS

	Intro to Academy 8 Sections Fundamental General Your first stop in Hack The Box Academy to become acquainted with the platform, its features, and its learning process.	100% Completed
	Learning Process 20 Sections Fundamental General The learning process is one of the essential and most important components that is often overlooked. This module does not teach you techniques to learn but describes the process of learning adapted to the field of information security. You will learn to understand how and when we learn best and increase and improve your learning efficiency greatly.	100% Completed
	Linux Fundamentals 30 Sections Fundamental General This module covers the fundamentals required to work comfortably with the Linux operating system and shell.	63.33% Completed
	Network Enumeration with Nmap 12 Sections Easy Offensive Nmap is one of the most used networking mapping and discovery tools because of its accurate results and efficiency. The tool is widely used by both offensive and defensive security practitioners. This module covers fundamentals that will be needed to use the Nmap tool for performing effective network enumeration.	75% Completed
	Introduction to Bash Scripting 10 Sections Easy General This module covers the basics needed for working with Bash scripts to automate tasks on Linux systems. A strong grasp of Bash is a fundamental skill for anyone working in a technical information security role. Through the power of automation, we can unlock the Linux operating system's full potential and efficiently perform habitual tasks.	30% Completed
	File Transfers 10 Sections Medium Offensive During an assessment, it is very common for us to transfer files to and from a target system. This module covers file transfer techniques leveraging tools commonly available across all versions of Windows and Linux systems.	100% Completed
	SQL Injection Fundamentals 17 Sections Medium Offensive Databases are an important part of web application infrastructure and SQL (Structured Query Language) to store, retrieve, and manipulate information stored in them. SQL injection is a code injection technique used to take advantage of coding vulnerabilities and inject SQL queries via an application to bypass authentication, retrieve data from the back-end database, or achieve code execution on the underlying server.	100% Completed



Web Requests

Web Requests

8 Sections Fundamental General

This module introduces the topic of HTTP web requests and how different web applications utilize them to communicate with their backends.

100% Completed



File Inclusion

File Inclusion

11 Sections Medium Offensive

File Inclusion is a common web application vulnerability, which can be easily overlooked as part of a web application's functionality.

100% Completed



Using the Metasploit Framework

Using the Metasploit Framework

15 Sections Easy Offensive

The Metasploit Framework is an open-source set of tools used for network enumeration, attacks, testing security vulnerabilities, evading detection, performing privilege escalation attacks, and performing post-exploitation.

73.33% Completed



Linux Privilege Escalation

Linux Privilege Escalation

28 Sections Easy Offensive

Privilege escalation is a crucial phase during any security assessment. During this phase, we attempt to gain access to additional users, hosts, and resources to move closer to the assessment's overall goal. There are many ways to escalate privileges. This module aims to cover the most common methods emphasizing real-world misconfigurations and flaws that we may encounter in a client environment. The techniques covered in this module are not an exhaustive list of all possibilities and aim to avoid extreme "edge-case" tactics that may be seen in a Capture the Flag (CTF) exercise.

28.57% Completed



Attacking Web Applications with Ffuf

Attacking Web Applications with Ffuf

13 Sections Easy Offensive

This module covers the fundamental enumeration skills of web fuzzing and directory brute forcing using the Ffuf tool. The techniques learned in this module will help us in locating hidden pages, directories, and parameters when targeting web applications.

76.92% Completed



Login Brute Forcing

Login Brute Forcing

13 Sections Easy Offensive

The module contains an exploration of brute-forcing techniques, including the use of tools like Hydra and Medusa, and the importance of strong password practices. It covers various attack scenarios, such as targeting SSH, FTP, and web login forms.

100% Completed



SQLMap Essentials

SQLMap Essentials

11 Sections Easy Offensive

The SQLMap Essentials module will teach you the basics of using SQLMap to discover various types of SQL Injection vulnerabilities, all the way to the advanced enumeration of databases to retrieve all data of interest.

100% Completed



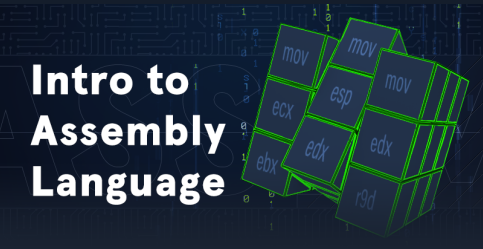
Introduction to Active Directory

Introduction to Active Directory

16 Sections Fundamental General

Active Directory (AD) is present in the majority of corporate environments. Due to its many features and complexity, it presents a vast attack surface. To be successful as penetration testers and information security professionals, we must have a firm understanding of Active Directory fundamentals, AD structures, functionality, common AD flaws, misconfigurations, and defensive measures.

87.5% Completed

	Introduction to Web Applications 17 Sections Fundamental General In the Introduction to Web Applications module, you will learn all of the basics of how web applications work and begin to look at them from an information security perspective.	100% Completed
	Getting Started 23 Sections Fundamental Offensive This module covers the fundamentals of penetration testing and an introduction to Hack The Box.	100% Completed
	Intro to Assembly Language 24 Sections Medium General This module builds the core foundation for Binary Exploitation by teaching Computer Architecture and Assembly language basics.	4.17% Completed
	Setting Up 22 Sections Fundamental General This module covers topics that will help us be better prepared before conducting penetration tests. Preparations before a penetration test can often take a lot of time and effort, and this module shows how to prepare efficiently.	31.82% Completed
	Penetration Testing Process 15 Sections Fundamental General This module teaches the penetration testing process broken down into each stage and discussed in detail. We will cover many aspects of the role of a penetration tester during a penetration test, explained and illustrated with detailed examples. The module also covers pre-engagement steps like the criteria for establishing a contract with a client for a penetration testing engagement.	100% Completed
	Cross-Site Scripting (XSS) 10 Sections Easy Offensive Cross-Site Scripting (XSS) vulnerabilities are among the most common web application vulnerabilities. An XSS vulnerability may allow an attacker to execute arbitrary JavaScript code within the target's browser and result in complete web application compromise if chained together with other vulnerabilities. This module will teach you how to identify XSS vulnerabilities and exploit them.	100% Completed
	Vulnerability Assessment 17 Sections Easy Offensive This module introduces the concept of Vulnerability Assessments. We will review the differences between vulnerability assessments and penetration tests, how to carry out a vulnerability assessment, how to interpret the assessment results, and how to deliver an effective vulnerability assessment report.	88.24% Completed
	Command Injections 12 Sections Medium Offensive Command injection vulnerabilities can be leveraged to compromise a hosting server and its entire network. This module will teach you how to identify and exploit command injection vulnerabilities and how to use various filter bypassing techniques to avoid security mitigations.	100% Completed



Using Web Proxies

Using Web Proxies

15 Sections Easy Offensive

Web application penetration testing frameworks are an essential part of any web penetration test. This module will teach you two of the best frameworks: Burp Suite and OWASP ZAP.

60% Completed



Footprinting

Footprinting

21 Sections Medium Offensive

This module covers techniques for footprinting the most commonly used services in almost all enterprise and business IT infrastructures. Footprinting is an essential phase of any penetration test or security audit to identify and prevent information disclosure. Using this process, we examine the individual services and attempt to obtain as much information from them as possible.

100% Completed



Attacking Common Applications

Attacking Common Applications

33 Sections Medium Offensive

Penetration Testers can come across various applications, such as Content Management Systems, custom web applications, internal portals used by developers and sysadmins, and more. It's common to find the same applications across many different environments. While an application may not be vulnerable in one environment, it may be misconfigured or unpatched in the next. It is important as an assessor to have a firm grasp of enumerating and attacking the common applications discussed in this module. This knowledge will help when encountering other types of applications during assessments.

69.7% Completed



Shells & Payloads

Shells & Payloads

17 Sections Medium Offensive

Gain the knowledge and skills to identify and use shells & payloads to establish a foothold on vulnerable Windows & Linux systems. This module utilizes a fictitious scenario where the learner will place themselves in the perspective of a sysadmin trying out for a position on CAT5 Security's network penetration testing team.

88.24% Completed



Attacking Common Services

Attacking Common Services

19 Sections Medium Offensive

Organizations regularly use a standard set of services for different purposes. It is vital to conduct penetration testing activities on each service internally and externally to ensure that they are not introducing security threats. This module will cover how to enumerate each service and test it against known vulnerabilities and exploits with a standard set of tools.

94.74% Completed



Web Attacks

Web Attacks

18 Sections Medium Offensive

This module covers three common web vulnerabilities, HTTP Verb Tampering, IDOR, and XXE, each of which can have a significant impact on a company's systems. We will cover how to identify, exploit, and prevent each of them through various methods.

100% Completed



Information Gathering - Web Edition

Information Gathering - Web Edition

19 Sections Easy Offensive

This module equips learners with essential web reconnaissance skills, crucial for ethical hacking and penetration testing. It explores both active and passive techniques, including DNS enumeration, web crawling, analysis of web archives and HTTP headers, and fingerprinting web technologies.

94.74% Completed



File Upload Attacks

11 Sections Medium Offensive

Arbitrary file uploads are among the most critical web vulnerabilities. These flaws enable attackers to upload malicious files, execute arbitrary commands on the back-end server, and even take control over the entire server and all web applications hosted on it and potentially gain access to sensitive data or cause a service disruption.

100% Completed

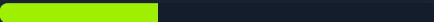


Active Directory Enumeration & Attacks

36 Sections Medium Offensive

Active Directory (AD) is the leading enterprise domain management suite, providing identity and access management, centralized domain administration, authentication, and much more. Due to the many features and complexity of AD, it presents a large attack surface that is difficult to secure properly. To be successful as infosec professionals, we must understand AD architectures and how to secure our enterprise environments. As Penetration testers, having a firm grasp of what tools, techniques, and procedures are available to us for enumerating and attacking AD environments and commonly seen AD misconfigurations is a must.

36.11% Completed



Password Attacks

26 Sections Medium Offensive

Passwords are still the primary method of authentication in corporate networks. If strong password policies are not enforced, users often choose weak, easy-to-remember passwords that can be cracked offline and leveraged to escalate access. As penetration testers, we encounter passwords in many forms during our assessments. It's essential to understand how passwords are stored, how they can be retrieved, methods for cracking weak passwords, techniques for using hashes that cannot be cracked, and how to identify weak or default password usage.

73.08% Completed

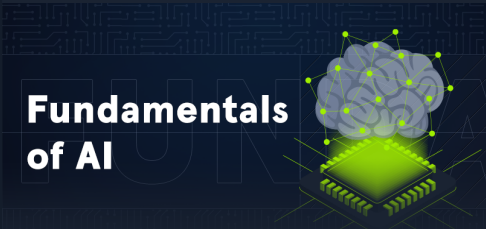


Pivoting, Tunneling, and Port Forwarding

18 Sections Medium Offensive

Once a foothold is gained during an assessment, it may be in scope to move laterally and vertically within a target network. Using one compromised machine to access another is called pivoting and allows us to access networks and resources that are not directly accessible to us through the compromised host. Port forwarding accepts the traffic on a given IP address and port and redirects it to a different IP address and port combination. Tunneling is a technique that allows us to encapsulate traffic within another protocol so that it looks like a benign traffic stream.

88.89% Completed



Fundamentals of AI

24 Sections Medium General

This module provides a comprehensive guide to the theoretical foundations of Artificial Intelligence (AI). It covers various learning paradigms, including supervised, unsupervised, and reinforcement learning, providing a solid understanding of key algorithms and concepts.

100% Completed



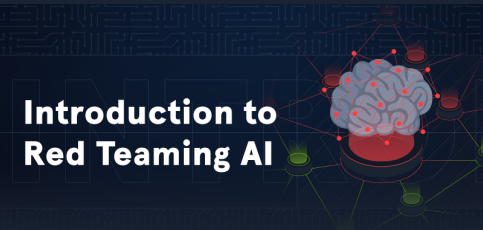
Applications of AI in InfoSec

25 Sections Medium General

This module is a practical introduction to building AI models that can be applied to various infosec domains. It covers setting up a controlled AI environment using Miniconda for package management and JupyterLab for interactive experimentation. Students will learn to handle datasets, preprocess and transform data, and implement structured workflows for tasks such as spam classification, network anomaly detection, and malware classification. Throughout the module, learners will explore essential Python libraries like Scikit-learn and PyTorch, understand effective approaches to dataset processing, and become familiar with common evaluation metrics, enabling them to navigate the entire lifecycle of AI model development and experimentation.

92% Completed



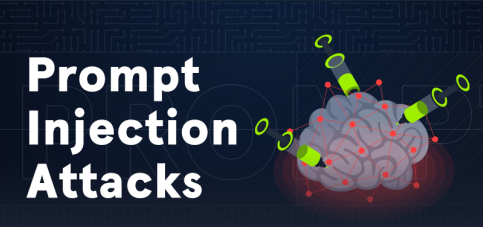


Introduction to Red Teaming AI

11 Sections Medium Offensive

This module provides a comprehensive introduction to the world of red teaming Artificial Intelligence (AI) and systems utilizing Machine Learning (ML) deployments. It covers an overview of common security vulnerabilities in these systems and the types of attacks that can be launched against their components.

100% Completed

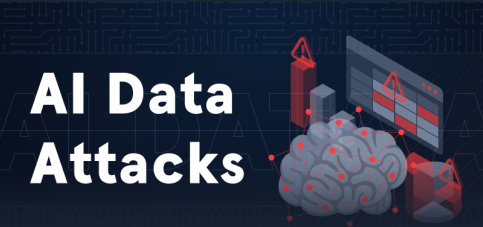


Prompt Injection Attacks

11 Sections Medium Offensive

This module comprehensively introduces one of the most prominent attacks on large language models (LLMs): Prompt Injection. It introduces prompt injection basics and covers detailed attack vectors based on real-world vulnerability reports. Furthermore, the module touches on academic research in the fields of novel prompt injection techniques and jailbreaks.

100% Completed

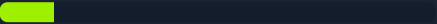


AI Data Attacks

25 Sections Hard Offensive

This module explores the intersection of Data and Artificial Intelligence, exposing how vulnerabilities within AI data pipelines can be exploited, ultimately aiming to degrade performance, achieve specific misclassifications, or execute arbitrary code.

12% Completed



LLM Output Attacks

14 Sections Medium Offensive

In this module, we will explore different LLM output vulnerabilities resulting from improper handling of LLM outputs and insecure LLM applications. We will also touch on LLM abuse attacks, such as hate speech campaigns and misinformation generation, with a particular focus on the detection and mitigation of these attacks.

100% Completed

